

# BUNDESREPUBLIK DEUTSCHLAND

GE998075  
#4



## CERTIFIED COPY OF PRIORITY DOCUMENT

**Bescheinigung**

JC 89 U.S. PTO  
09/459290  
12/17/99

Die Firma International Business Machines Corp. in Armonk, N.Y./N.Y.A. hat eine Patentanmeldung unter der Bezeichnung

"Vorrichtung und Verfahren zum Verwalten von Identifikationsmerkmalen"

am 16. Januar 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 06 F und G 07 G der Internationalen Patentklassifikation erhalten.

München, den 26. September 1999

**Deutsches Patent- und Markenamt**

**Der Präsident**

Im Auftrag

Nietledt

Aktenzeichen: 199 01 523.6

## B E S C H R E I B U N G

**Vorrichtung und Verfahren zum Verwalten von  
Identifikationsmerkmalen**

Die Erfindung betrifft eine Vorrichtung und ein Verfahren zum Verwalten von Identifikationsmerkmalen. Insbesondere betrifft die Erfindung eine Vorrichtung und ein Verfahren zum Anlegen und/oder Ändern von Identifikationsmerkmalen.

Zur Kontrolle des Zugangs von Personen zu Systemen, wie Personalcomputern, Rechnernetzen, Gebäuden, Räumen etc., werden häufig Identifikationsmerkmale, wie beispielsweise Paßwörter, PIN-Kennwörter, biometrische Merkmale oder Stimmerkmale, verwendet, die von den Personen zum Zwecke ihrer Identifizierung einer Kontrollvorrichtung mitgeteilt werden, um einen Zugang zu einem System (Computersystem, Gebäudezugangssystem, ...) zu erlangen. Neben der Neuanlegung von solchen Identifikationsmerkmalen für jeden neuen Benutzer des Systems müssen diese Identifikationsmerkmale aus Sicherheitsgründen von Zeit zu Zeit geändert werden. Verfahren zum Anlegen und Ändern von Identifikationsmerkmalen sind bekannt. Bei diesen Verfahren hat der Benutzer während der gesamten Dauer der Eingabe des neuen Identifikationsmerkmals die Möglichkeit, die Eingabe abzuschließen. Eine Prüfung des eingegebenen neuen Identifikationsmerkmals findet erst statt, nachdem die Eingabe durch den Benutzer abgeschlossen wird. Häufig wird auch das neue Identifikationsmerkmal zweimal eingegeben, um versehentliche Fehleingaben bzw. biometrische Erkennungsfehler, im folgenden zusammenfassend als Fehleingaben bezeichnet, zu vermeiden. Auch hier findet eine Prüfung der Identifikationsmerkmale erst nach der Eingabe beider Identifikationsmerkmale und dem Abschließen der Eingabe durch den Benutzer statt.

Erfüllt das neue Identifikationsmerkmal bestimmte zuvor festgelegte Kriterien nicht, so kommt es zu einem Fehlversuch. Ebenso führen Fehleingaben, d.h. versehentliche oder technisch bedingte Differenzen zwischen dem neu anzulegenden Identifikationsmerkmal und dessen Wiederholung, zu einem Fehlversuch. Diese Fehlversuche führen im allgemeinen zu Fehlermeldungen. Darüber hinaus können sie auch zu einer Sperrung der Zugriffsrechte des Benutzers führen. Dadurch ist die Benutzerfreundlichkeit beim Anlegen und Ändern von Identifikationsmerkmalen stark eingeschränkt.

Der Erfindung liegt die Aufgabe zugrunde, die Benutzerfreundlichkeit beim Anlegen und Ändern von Identifikationsmerkmalen zu erhöhen.

Erfindungsgemäß wird diese Aufgabe durch die unabhängigen Ansprüche gelöst.

Die Erfindung beruht auf dem Gedanken, eine Prüfung des neuen Identifikationsmerkmals während seiner Bereitstellung durchzuführen, und das Identifikationsmerkmal erst dann an eine das Identifikationsmerkmal weiterverarbeitende Vorrichtung zu übergeben, wenn alle Prüfkriterien erfüllt sind.

Durch die vorliegende Erfindung wird die Benutzerfreundlichkeit beim Verwalten, und insbesondere beim Anlegen und Ändern von Identifikationsmerkmalen wesentlich verbessert, da Fehlversuche bei der Bereitstellung des neuen Identifikationsmerkmals vermieden werden. Das betrifft sowohl Fehlversuche aufgrund der Bereitstellung eines Identifikationsmerkmals, welches nicht bestimmten Kriterien genügt, als auch Fehlversuche, die durch eine Fehleingabe bei einer möglichen zweiten Bereitstellung des Identifikationsmerkmals entstehen können. Die Erfindung kann auf sämtliche Arten von Identifikationsmerkmalen

angewendet werden, insbesondere auf Paßwörter, PIN-Kennwörter, biometrische Merkmale (Fingerprintsan, Gesichtsscan, Augenscan, ...), Stimmerkmale, etc. Durch das Wegfallen der Fehlversuche und der damit verbundenen Systemaktionen, wie Fehlermeldungen, Sperrung oder Löschung der Zugriffsrechte des Benutzers, wird das Anlegen und Ändern von Identifikationsmerkmalen einfacher, schneller und sicherer.

Die Erfindung ist nachstehend anhand von Beispielen näher beschrieben.

Fig.1 zeigt einen Personalcomputer, bestehend aus Systemeinheit, Tastatur, Maus und Monitor für den Gebrauch mit einem bevorzugten Ausführungsbeispiel der Erfindung.

Fig.2 zeigt eine Eingabemaske in Form einer graphische Benutzerschnittstelle für das Ändern von Paßwörtern für den Gebrauch mit einem bevorzugten Ausführungsbeispiel der Erfindung.

Die Figuren 3a bis 3e zeigen Flußdiagramme, die das Verfahren eines bevorzugten Ausführungsbeispiels der Erfindung darstellen.

Zum Zwecke der Vereinfachung wird die Erfindung nachfolgend lediglich am Beispiel der Änderung eines Paßwortes beschrieben. Die Erfindung ist jedoch nicht auf die Änderung von Paßwörtern beschränkt. Ebenso kann sie für das Neuanlegen von Paßwörtern sowie zur Änderung und Neuanlegung von beliebigen anderen Identifikationsmerkmalen verwendet werden.

Ein Ausführungsbeispiel der Erfindung kann in einer beliebigen Rechnersystemumgebung, mit einer beliebigen Hardware oder mit einer beliebigen Kombination von Hardware

und Software implementiert werden. Nachfolgend wird die Erfindung am Beispiel der Änderung eines Paßwortes für einen Personalcomputer erläutert.

In Fig.1 ist ein solcher Personalcomputer 10 für die Implementierung der Erfindung dargestellt, der aus einer Systemeinheit 11, einer Tastatur 12, einer Maus 13 und einem Monitor 14 besteht. Der Bildschirm 15 des Monitors 14 wird verwendet, um eine graphische Benutzerschnittstelle darzustellen. Die graphische Benutzerschnittstelle wird von dem Betriebssystem des Personalcomputers 10 unterstützt, so daß ein Benutzer die Tastatur 12 und die Maus 13 verwenden kann, um Daten, wie zum Beispiel Paßwörter, in den Personalcomputer einzugeben oder Benutzeraktionen ausführen zu können. Der Personalcomputer 10 beinhaltet weiterhin wenigstens einen Prozessor zum Verarbeiten von Informationen, sowie einen Speicher, in dem Daten abgelegt werden können. Als Betriebssystem kann beispielsweise IBM OS/2 verwendet werden.

Der Ablauf des Verfahrens eines bevorzugten Ausführungsbeispiels der Erfindung ist anhand von Flußdiagrammen in den Figuren 3a bis 3e beschrieben.

Der Personalcomputer 10 verfügt zum Ändern des Paßwortes über eine Vorrichtung zum Ändern von Paßwörtern. Die Vorrichtung zum Ändern von Paßwörtern kann als Datenverarbeitungsprogramm (Software) geschrieben worden sein. In diesem Fall wird das Programm nach dem Aufruf im Prozessor des Personalcomputers 10 ausgeführt. Die Vorrichtung zum Ändern von Paßwörtern kann jedoch auch in Form von Hardware implementiert sein, beispielsweise festverdrahtet im Personalcomputer 10.

Wie in Fig. 3a dargestellt, startet der Benutzer in einem ersten Schritt 3000 ein Programm zum Ändern von Paßwörtern

entsprechend der vorliegenden Erfindung. Dieses stellt dem Benutzer eine Eingabemaske 20 in Form einer graphischen Benutzerschnittstelle zur Verfügung, welcher in einem Schritt 3010 auf dem Bildschirm 15 erscheint. Ein Beispiel für eine solche Eingabemaske 20 ist in Fig.2 dargestellt.

Die Eingabemaske 20 beinhaltet ein erstes Eingabefeld 21 zur Eingabe des neuen Paßwortes sowie ein zweites Eingabefeld 22 zur wiederholten Eingabe des neuen Paßwortes. Außerdem beinhaltet sie eine Möglichkeit zum Abschließen der Eingabe, hier in Form einer „OK“-Schaltfläche 23, sowie eine Möglichkeit zum Abbrechen der Eingabe, hier in Form einer „Abbruch“-Schaltfläche 24.

Nach dem Erscheinen der Eingabemaske 20 auf dem Bildschirm 15 ist die „OK“-Schaltfläche nicht betätigbar. Die Schaltfläche ist dann derart dargestellt, daß der Benutzer erkennen kann, daß sie nicht betätigbar ist. Üblicherweise geschieht das durch eine Schattierung der Schaltfläche.

Das Programm zum Ändern von Paßwörtern überprüft in Schritt 3020, ob der Benutzer die „Abbruch“-Schaltfläche 24 betätigt. Ist das der Fall, so wird, wie in Fig.3e gezeigt, die Eingabemaske geschlossen, Schritt 3160, und das Verfahren zum Ändern des Paßwortes wird mit Schritt 3170 beendet.

Wird die „Abbruch“-Schaltfläche 24 nicht betätigt, so prüft das Programm zum Ändern von Paßwörtern in Schritt 3030, ob ein Zeichen in das erste Eingabefeld 21 der Eingabemaske 20 eingetragen wird.

Ist die Eingabemaske 20 aktiv, so wird jeder Tastendruck vom Betriebssystem an das Programm zum Ändern von Paßwörtern übergeben. Dazu wird das Programm zum Ändern von Paßwörtern dem Betriebssystem als zuständige Handleroutine angemeldet.

Gibt der Benutzer jetzt mittels der Tastatur 12 ein Zeichen in das erste Eingabefeld ein, so wird, wie in Fig.3b beschrieben, in Schritt 3060 das eingegebene Zeichen unter der Bezeichnung PASSWORT\_1 in einen Pufferspeicher des Personalcomputers 10 abgelegt bzw. das eingegebene Zeichen an ein schon bestehendes PASSWORT\_1 angehängt. Zuvor prüft das Programm zum Ändern von Paßwörtern in Schritt 3040, ob mit dem letzten Tastendruck des Benutzers die Taste "Backspace" gedrückt wurde. Ist das der Fall, wird in Schritt 3050 das letzte Zeichen von PASSWORT\_1 im Pufferspeicher gelöscht, und auf die Eingabe eines weiteren Zeichens gewartet.

Anschließend wird in Schritt 3070 das eingegebene Zeichen durch das Betriebssystems des Rechners in das erste Eingabefeld 21 der Eingabemaske 20 eingetragen. Vorzugsweise wird dabei nur ein Platzhalter, beispielsweise das Zeichen "\*", eingetragen, um das Paßwort auf dem Bildschirm 15 unlesbar darzustellen.

Nachfolgend wird das eingegebene Zeichen durch das Betriebssystem des Personalcomputers 10 einer Vorrichtung zur Prüfung des Paßwortes (Prüfvorrichtung) übergeben.

Die Vorrichtung zur Prüfung des Paßwortes prüft einzeln jedes durch den Benutzer neu eingegebene Zeichen dahingehend, ob das sich aus den eingegebenen Zeichen ergebende Paßwort bestimmten Prüfkriterien, im folgenden als Kriterien bezeichnet, entspricht. Diese Prüfung erfolgt bevorzugt während der Eingabe des Paßwortes.

Kriterien für neue Paßwörter können beispielsweise sein: Mindestlänge und/oder Höchstlänge des Paßwortes, Vorgaben, welche Zeichen in einem Paßwort enthalten sein müssen, Vorgaben, welche Zeichen in einem Paßwort nicht enthalten sein dürfen, Übereinstimmung des neuen Paßwortes mit einem

vorherigen Paßwort des Benutzers, Übereinstimmung des neuen Paßwortes mit Paßwörtern von anderen Benutzern etc.

Im Allgemeinen sind die Kriterien von dem jeweiligen System (Computersystem, Gebäudezugangssystem) abhängig und daher beliebig wählbar. Da die Erfindung nicht auf Paßwörter beschränkt ist, sondern beispielsweise auch für biometrische Identifikationsmerkmale (Fingerprint, Gesichtsscan, Augenscan, ...) einsetzbar ist, kann ein Kriterium beispielsweise auch die Vollständigkeit der eingelesenen Informationen (z.B. Vorhandensein einer vorgeschriebene Mindestanzahl von Knotenpunkten bei Fingerprints) sein.

In dem vorliegendem Beispiel soll das neue Paßwort aus fünf Zeichen bestehen, wobei es sich aus drei Buchstaben und zwei Ziffern zusammensetzen muß. Weiterhin soll das erste Zeichen des Paßwortes ein Buchstabe sein. Ein weiteres Kriterium ist die Übereinstimmung der wiederholten Eingabe des neuen Paßwortes in das zweite Eingabefeld (PASSWORT\_2) mit dem in das erste Eingabefeld eingetragenen Paßwort (PASSWORT\_1).

In einer Ausführungsform der Erfindung ist die Vorrichtung zur Prüfung des Paßwortes Bestandteil des Programms zum Ändern von Paßwörtern und die zu prüfenden Kriterien sind in dem Programmcode des Programms zum Ändern von Paßwörtern enthalten.

Wie in Fig.3d dargestellt, prüft das Programm zum Ändern von Paßwörtern nacheinander alle Kriterien, die für dieses Beispiel bestimmt worden sind. Zunächst wird im Schritt 3080 geprüft, ob das im Pufferspeicher abgelegte PASSWORT\_1 fünf Zeichen enthält. Ist dies nicht der Fall, so sendet das Programm zum Ändern von Paßwörtern in Schritt 3130 an die „OK“-Schaltfläche 23 ein Signal zur Deaktivierung der Schaltfläche 23 über die entsprechende Betriebssystem-

schnittstelle. Der Benutzer kann demnach die Eingabe in die Eingabemaske 20 nicht abschließen.

In dem Fall, daß das erste Kriterium erfüllt ist, überprüft das Programm zum Ändern von Paßwörtern in Schritt 3090 das nächste Kriterium, nämlich, ob das PASSWORT\_1 drei Buchstaben und zwei Ziffern enthält. Ist dieses Kriterium nicht erfüllt, erfolgt wiederum eine Deaktivierung der „OK“-Schaltfläche 23 in Schritt 3130. Sollte dieses Kriterium erfüllt sein, so werden in den Schritten 3100 und 3110 nacheinander die weiteren Kriterien geprüft, wobei bei der Nichterfüllung eines der Kriterien die Prüfung des neu eingegebenen Zeichens jeweils mit der Deaktivierung der „OK“-Schaltfläche 23 abgeschlossen wird.

Wird in Schritt 3030 (Fig. 3a) festgestellt, daß kein Zeichen in das erste Eingabefeld 21 eingegeben wird, so wird in Schritt 3031 geprüft, ob ein Zeichen in das zweite Eingabefeld 22 der Eingabemaske 20 eingegeben wird. Ist das der Fall, so wird, wie in Fig. 3c beschrieben, analog zu den Schritten 3040, 3050, 3060 und 3070 verfahren. Dabei wird in Schritt 3061 das eingegebene Zeichen unter der Bezeichnung PASSWORT\_2 in den Pufferspeicher des Personalcomputers 10 abgelegt bzw. das eingegebene Zeichen an ein schon bestehendes PASSWORT\_2 angehängt. Zuvor prüft das Programm zum Ändern von Paßwörtern in Schritt 3041, ob mit dem letzten Tastendruck des Benutzers die Taste „Backspace“ gedrückt wurde. Ist das der Fall, wird in Schritt 3051 das letzte Zeichen von PASSWORT\_2 im Pufferspeicher gelöscht.

Anschließend wird in Schritt 3071 das eingegebene Zeichen durch das Betriebssystems des Rechners in das zweite Eingabefeld 22 der Eingabemaske 20 eingetragen. Vorzugsweise wird dabei nur ein Platzhalter, beispielsweise das Zeichen „\*“, eingetragen, um das Paßwort auf dem Bildschirm 15 unlesbar darzustellen.

Wie bei der Eingabe eines Zeichens in das erste Eingabefeld 21 wird auch bei der Eingabe eines Zeichens in das zweite Eingabefeld 22 das eingegebene Zeichen durch das Betriebssystem des Personalcomputers 10 jetzt der Vorrichtung zur Prüfung des Paßwortes übergeben, die prüft, ob das sich aus den eingegebenen Zeichen ergebende Paßwort bestimmten Kriterien entspricht. Wie oben beschrieben, wird diese Prüfung in dem vorliegenden Beispiel durch das Programm zum Ändern von Paßwörtern beginnend mit dem Schritt 3080, Fig.3d, durchgeführt. Für den Fall, daß eines der Kriterien nicht erfüllt ist, endet die Prüfung des eingegebenen Zeichens mit Schritt 3130, der Deaktivierung der „OK“-Schaltfläche 23 in der Eingabemaske 20.

Nach der Deaktivierung der „OK“-Schaltfläche 23 in Schritt 3130 läuft das Verfahren mit den Schritten 3020, 3030, ... (Fig.3a) weiter, d.h. das Programm zum Ändern von Paßwörtern wartet auf weitere Eingaben des Benutzers.

Nach jeder Eingabe eines neuen Zeichens werden die oben beschriebenen Verfahrensschritte durchlaufen und das Programm zum Ändern von Paßwörtern prüft, ob die vorgegebenen Kriterien erfüllt sind. Solange dies nicht der Fall ist, wird in Schritt 3130 das Signal zur Deaktivierung der „OK“-Schaltfläche 23 gesendet, und der Benutzer kann die Eingabe in die Eingabemaske 20, und damit die Änderung des Paßwortes, nicht mit der „OK“-Schaltfläche 23 abschließen.

Wird bei der Prüfung der Kriterien festgestellt, daß alle Kriterien erfüllt sind, so wird die Prüfung der eingegebenen Zeichen mit Schritt 3120 (Fig.3d) abgeschlossen.

Da alle Kriterien erfüllt sind, wird dem Benutzer die Möglichkeit gegeben, die Eingabe des Paßwortes abzuschließen. Dazu sendet das Programm zum Ändern von Paßwörtern über die entsprechende Betriebssystem-

schnittstelle ein Signal zur Aktivierung an die „OK“-Schaltfläche 23 in der Eingabemaske 20. Nach der Aktivierung der „OK“-Schaltfläche 23 ist sie derart dargestellt, daß der Benutzer erkennen kann, daß sie nicht mehr deaktiviert ist. Die üblicherweise vorhandene Schattierung der Schaltfläche ist dann aufgehoben.

Die „OK“-Schaltfläche 23, dargestellt in Fig.2, kann dann von dem Benutzer betätigt werden. Sie kann so ausgeführt sein, daß die Betätigung mit Hilfe der Maus 13 oder der Tastatur 12 erfolgen kann.

Wie in Fig.3e dargestellt, prüft das Programm zum Ändern von Paßwörtern in Schritt 3140, ob die „OK“-Schaltfläche 23 betätigt wird. Ist dies der Fall, so übergibt das Programm zum Ändern von Paßwörtern in Schritt 3150 das neue Paßwort (PASSWORT\_1) über eine entsprechende Funktion an ein das Paßwort weiterverarbeitendes System des Personalcomputers 10. Anschließend wird die Eingabemaske 20 in Schritt 3160 geschlossen, und das Programm zum Ändern von Paßwörtern in Schritt 3170 beendet.

Wurde das Paßwort an das das Paßwort weiterverarbeitende System des Personalcomputers 10 übergeben, so verarbeitet dieses das neue Paßwort des Benutzers. Beispielsweise kann die Überprüfung weiterer Paßwortkriterien, Speicherung des Paßwortes in dafür vorgesehene Datenspeicher oder die Weitergabe des Paßwortes an weitere Systemeinheiten oder andere Rechner in einem Rechnernetz erfolgen.

Der Benutzer weiß bis zu dem Zeitpunkt, an dem alle Kriterien erfüllt sind, nicht, ob das von ihm eingegebene Paßwort akzeptiert werden wird. Erst wenn alle Kriterien erfüllt sind, ist die Eingabe des Identifikationsmerkmals in die Eingabemaske 20 abschließbar. Dann jedoch kann der Benutzer sicher sein, daß das von ihm eingegeben Paßwort den

Anforderungen des Systems genügt, und die Eingabe des Paßwortes abgeschlossen werden kann.

Ist ein manuelles Abschließen der Eingabe des neuen Paßwortes durch den Benutzer vorgesehen, so werden mit der vorliegenden Erfindung Fehlversuche mit Hilfe der Aktivierung bzw. Deaktivierung der „OK“-Schaltfläche 23 in der Eingabemaske 20 vermieden. Der Benutzer bekommt erst dann die Möglichkeit, seine Eingabe abzuschließen, wenn eine Prüfung des eingegebenen Paßwortes erfolgreich durchgeführt wurde.

In einer weiteren Ausführungsform erfolgt das Abschließen der Eingabe in die Eingabemaske 20 ohne Einfluß des Benutzers, sobald die Eingabe des neuen Identifikationsmerkmals abgeschlossen ist, und das neue Identifikationsmerkmal alle an es gestellten Kriterien erfüllt. Ein derartiges automatisches Abschließen der Eingabe, das von einer Systemkomponente durchgeführt werden kann, ist vor allem bei biometrischen Identifikationsmerkmalen, beispielsweise bei dem Abtasten von Fingerlinien sinnvoll. Sollte ein Identifikationsmerkmal nicht korrekt eingegeben worden sein, könnte das System, gegebenenfalls auch mehrmals, zu einer erneuten Eingabe des Identifikationsmerkmals auffordern. Fehlversuche des Benutzers werden somit vermieden.

Während der Benutzer in den vorherigen Ausführungsbeispielen während der gesamten Eingabe des neuen Paßwortes nicht nachvollziehen kann, zu welchem Zeitpunkt die von ihm eingegebenen Zeichen den zu prüfenden Kriterien genügen, wird in einer weiteren bevorzugten Ausführungsform der Erfindung, zusätzlich zur Aktivierung/Deaktivierung der Möglichkeit des Abschließens der Eingabe in die Eingabemaske 20, ein Fehlerindikator aktiviert. Dieser informiert den Benutzer darüber, ob die von der Anwendung geforderten

Kriterien zum Anlegen bzw. Ändern von Paßwörtern erfüllt sind. Fehlerindikatoren können sein: Ampeldarstellungen, Flaggendarstellungen, definierte Signaldarstellungen, akustische Warntöne, Farbindikatoren (LED, Segmentanzeigen, ...), etc. Bei dem Abschließen der Eingabe des Identifikationsmerkmals ohne Einfluß des Benutzers kann ein solchen Fehlerindikator auch alternativ zu der Möglichkeit des Abschließens der Eingabe des Identifikationsmerkmals vorgesehen sein.

Um eine mißbräuchliche Verwendung des Verfahrens, insbesondere das Ausspähen von aktuell gültigen Kriterien der Paßwörter zu verhindern, kann in einem weiteren Ausführungsbeispiel mittels bekannter Verfahren während der Eingabe des neuen Paßwortes überprüft werden, wie stark ein eingegebenes Paßwort von den vorgegebenen Kriterien abweicht. Diese Überprüfung kann im Rahmen der Prüfung der Kriterien erfolgen. Wird ein definierter Abweichungsgrad überschritten, wird die Eingabe des Paßwortes abgebrochen. Der erlaubte Abweichungsgrad ist von der jeweiligen Anwendung abhängig und daher beliebig wählbar.

Obwohl bisher immer von einer zweimaligen Eingabe des Paßwortes ausgegangen wurde, ist die Erfindung nicht darauf beschränkt. In einer weiteren Ausführungsform der Erfindung beinhaltet die Eingabemaske 20 lediglich ein einziges Eingabefeld zur Eingabe des neuen Paßwortes. Eine Wiederholung der Eingabe des neuen Paßwortes ist nicht vorgesehen.

In noch einer weiteren Ausführungsform ist eine mehrmalige, beispielsweise dreifache oder vierfache, Eingabe des Paßwortes vorgesehen. Bevorzugt ist dann, wie auch bei der zweifachen Eingabe des Paßwortes, ein Kriterium während der Prüfung die Übereinstimmung der eingegebenen Paßwörter.

Die Erfindung ist nicht auf eine spezielle Methode der Bereitstellung des Identifikationsmerkmals beschränkt. Die Bereitstellung der Identifikationsmerkmale kann, wie in den obengenannten Beispielen, durch Eingabe über eine Tastatur erfolgte. Identifikationsmerkmale können jedoch auch anders bereitgestellt werden, zum Beispiel durch die Übermittlung eines gesprochenen Wortes, beispielsweise mittels eines Mikrophones, das Abtasten einer Pupille, beispielsweise mittels einer optischen Abtastvorrichtung, das Lesen eines Fingerabdruckes, beispielsweise mittels optoelektronischer Leseeinheiten etc.

## P A T E N T A N S P R Ü C H E

1. Verfahren zum Verwalten von Identifikationsmerkmalen in einem Computer mit den Schritten:
  - Bereitstellen des Identifikationsmerkmals durch einen Benutzer,
  - Prüfen des Identifikationsmerkmals durch eine Prüfvorrichtung während des Bereitstellens, wobei die Erfüllung mindestens eines Prüfkriteriums geprüft wird,
  - Übergeben des Identifikationsmerkmals an eine das Identifikationsmerkmal weiterverarbeitende Vorrichtung, wenn das Identifikationsmerkmal alle Prüfkriterien erfüllt.
2. Verfahren nach Anspruch 1 mit dem zusätzlichen Schritt:
  - Informieren des Benutzers während des Bereitstellens darüber, ob das Identifikationsmerkmal die Prüfkriterien erfüllt.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß das Informieren des Benutzers dadurch erfolgt, daß dem Benutzer eine Möglichkeit zum Abschließen der Bereitstellung des Identifikationsmerkmals zur Verfügung gestellt wird, und diese Möglichkeit deaktiviert wird, wenn das Identifikationsmerkmal wenigstens ein Prüfkriterium nicht erfüllt, und diese Möglichkeit aktiviert wird, wenn das Identifikationsmerkmal alle Prüfkriterien erfüllt, und das Identifikationsmerkmal nur dann an die das Identifikationsmerkmal weiterverarbeitende Vorrichtung übergeben wird, wenn das Bereitstellen abgeschlossen ist.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß, wenn das Identifikationsmerkmal

aus mehreren Komponenten besteht, das Prüfen für jede Komponente einzeln erfolgt.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß während des Prüfens die Abweichung des Identifikationsmerkmals von den Prüfkriterien festgestellt wird, und der Bereitstellungsvorgang abgebrochen wird, wenn ein bestimmter Abweichungsgrad überschritten wird.
6. Vorrichtung zum Verwalten von Identifikationsmerkmalen in einem Computer, dadurch gekennzeichnet, daß sie umfaßt:
  - Mittel zum Bereitstellen des Identifikationsmerkmals durch einen Benutzer,
  - Prüfvorrichtung zum Prüfen des Identifikationsmerkmals während des Bereitstellens auf Erfüllung mindestens eines Prüfkriteriums,
  - Mittel zum Übergeben des Identifikationsmerkmals an eine das Identifikationsmerkmal weiterverarbeitende Vorrichtung.
7. Vorrichtung nach Anspruch 6, dadurch gekennzeichnet, daß sie Mittel zum Informieren des Benutzers darüber umfaßt, ob das Identifikationsmerkmal die Prüfkriterien erfüllt.
8. Vorrichtung nach einem der Ansprüche 6 oder 7, dadurch gekennzeichnet, daß sie umfaßt:
  - eine Möglichkeit zum Abschließen der Bereitstellung des Identifikationsmerkmals durch den Benutzer,
  - Mittel zum Deaktivieren dieser Möglichkeit,
  - Mittel zum Aktivieren dieser Möglichkeit.
9. Vorrichtung nach einem der Ansprüche 6 bis 8, dadurch gekennzeichnet, daß, wenn das Identifikationsmerkmal

aus mehreren Komponenten besteht, sie Mittel zum einzelnen Prüfen jeder Komponente umfaßt.

10. Vorrichtung nach einem der Ansprüche 6 bis 9, dadurch gekennzeichnet, daß sie Mittel umfaßt, die eine Abweichung des Identifikationsmerkmals von den Prüfkriterien feststellen, und weiterhin Mittel umfaßt, die den Bereitstellungsvorgang abbrechen, wenn ein bestimmter Abweichungsgrad überschritten wird.

## Z U S A M M E N F A S S U N G

Die Erfindung betrifft eine Vorrichtung und ein Verfahren zum Verwalten, insbesondere zum Anlegen und Ändern, von Identifikationsmerkmalen.

Während der Bereitstellung des neuen Identifikationsmerkmals durch einen Benutzer wird eine Prüfung des Identifikationsmerkmals durchgeführt. In Abhängigkeit von dem Ergebnis dieser Prüfung wird eine Möglichkeit des Abschließens der Eingabe des neuen Identifikationsmerkmals aktiviert bzw. deaktiviert.

Die Benutzerfreundlichkeit beim Anlegen und Ändern von Identifikationsmerkmalen wird wesentlich verbessert, da Fehlversuche bei der Eingabe von neuen Identifikationsmerkmalen vermieden werden.

(Fig. 3d)

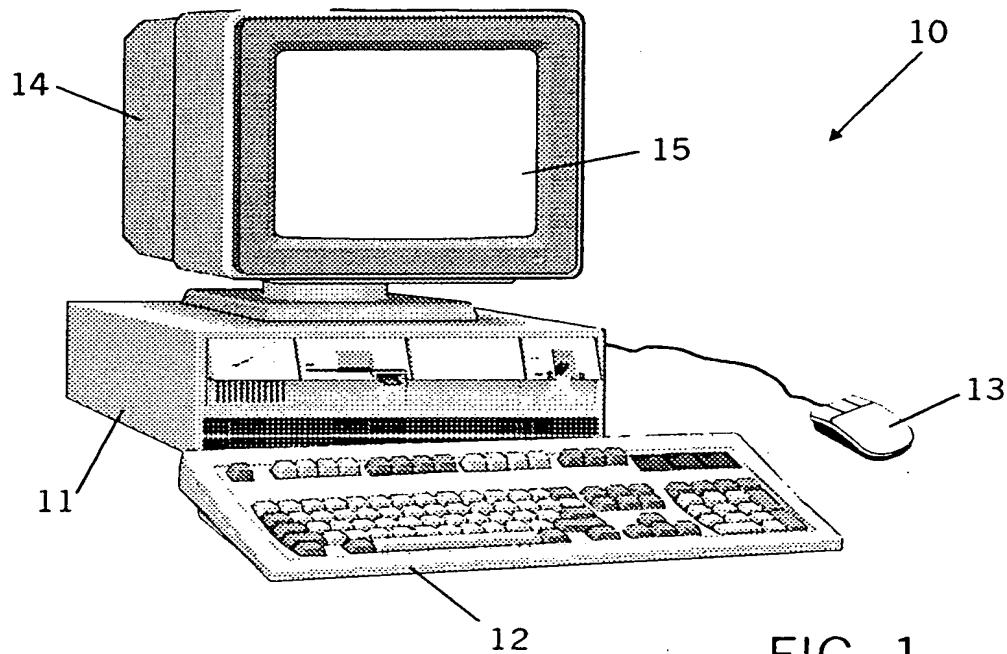


FIG. 1

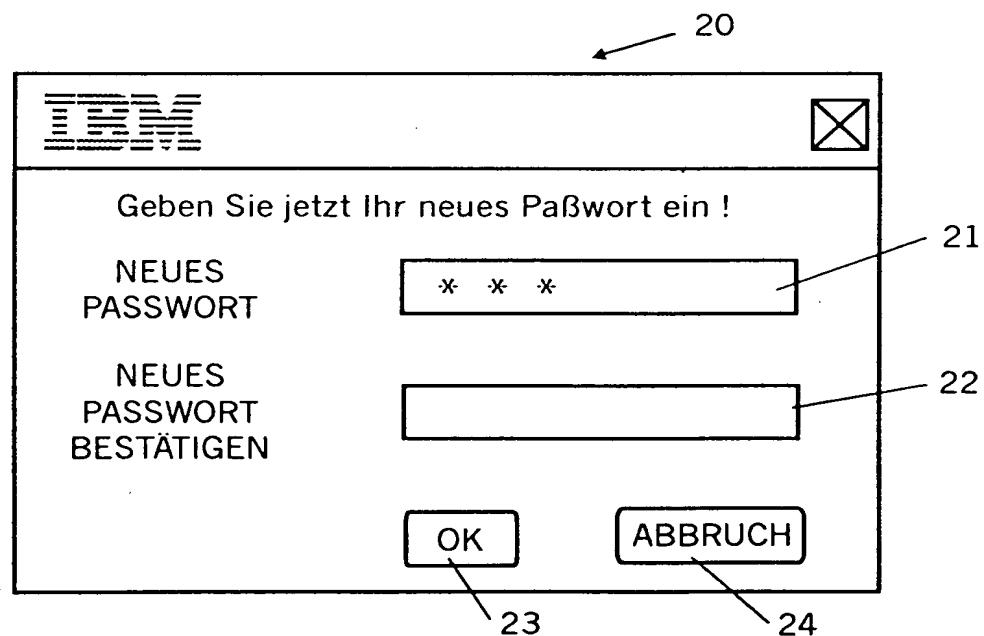


FIG. 2

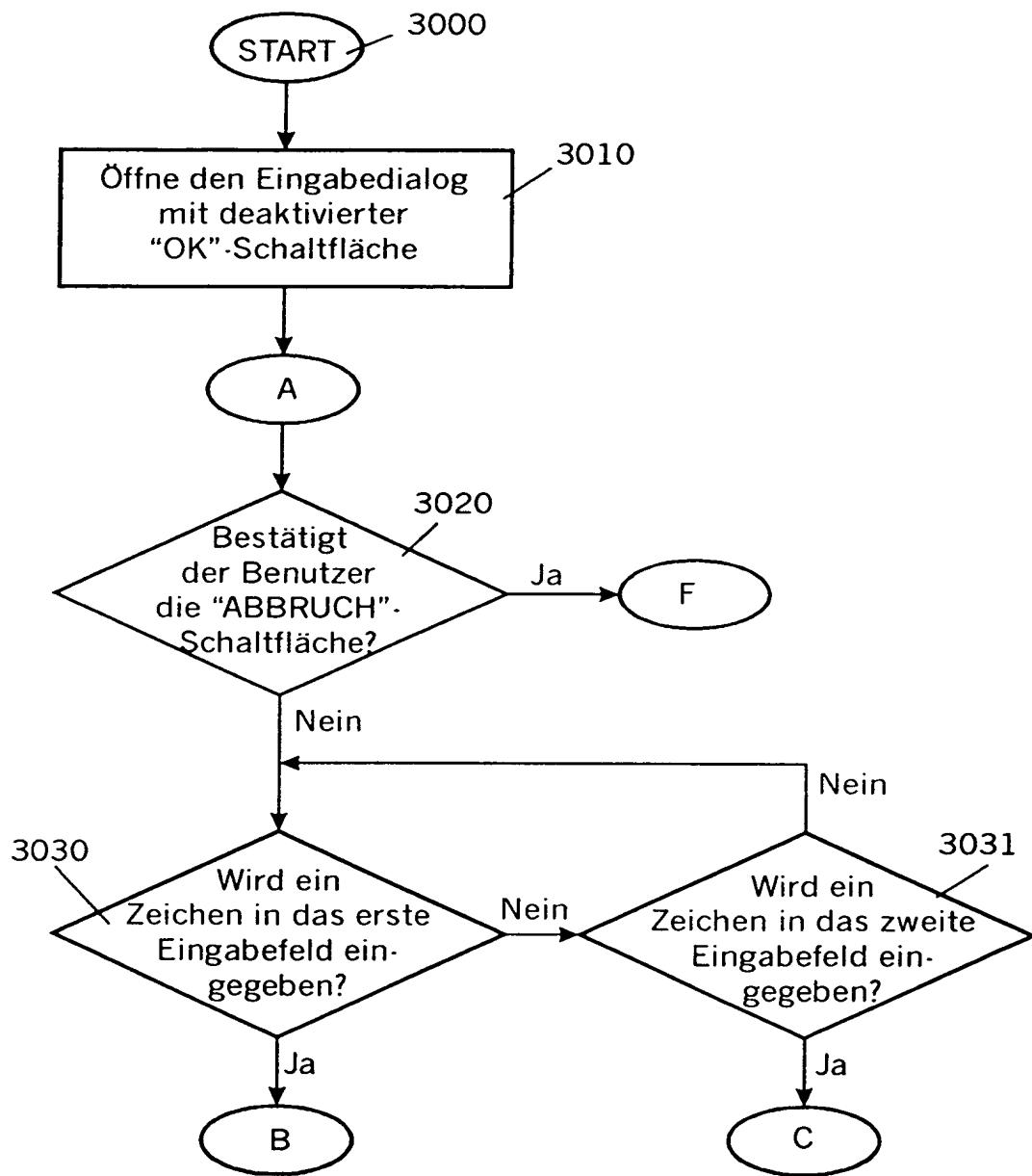


FIG. 3A

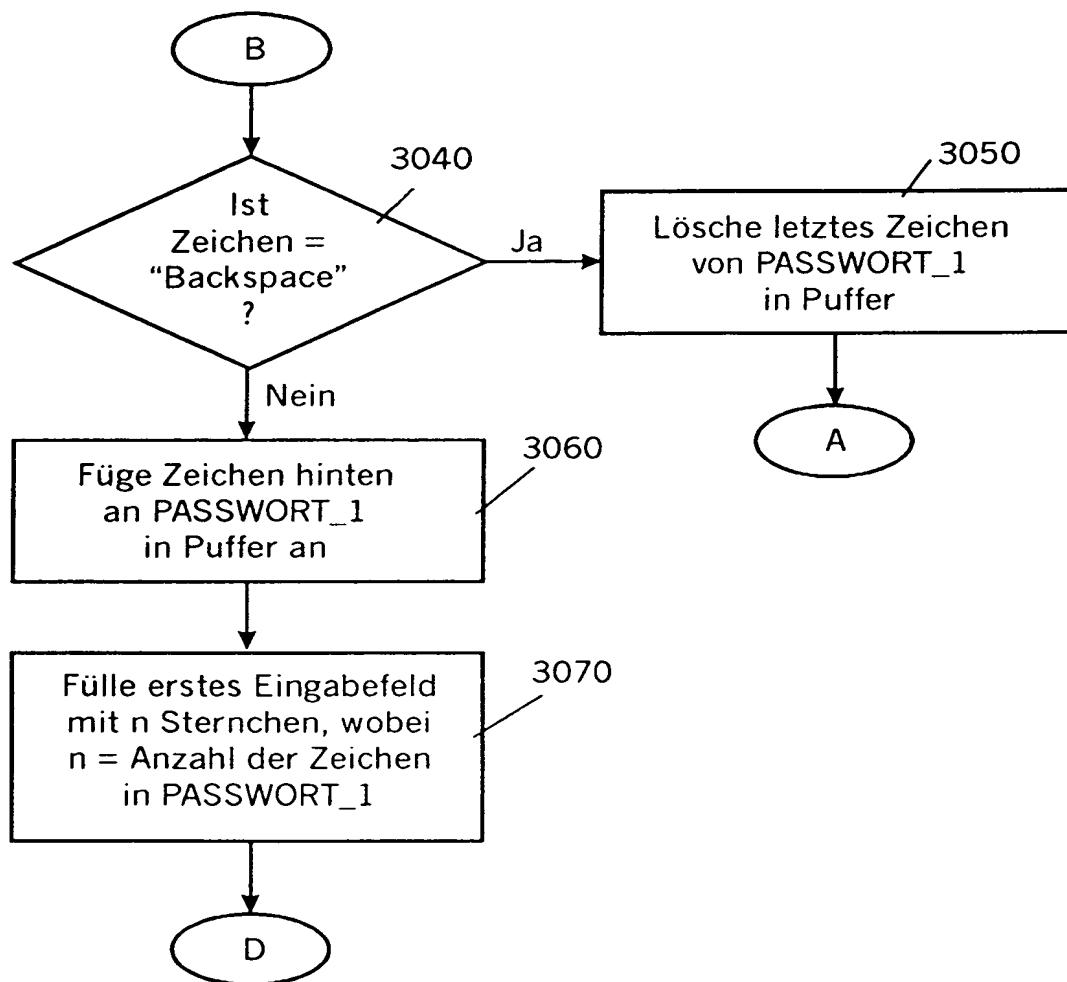


FIG. 3B

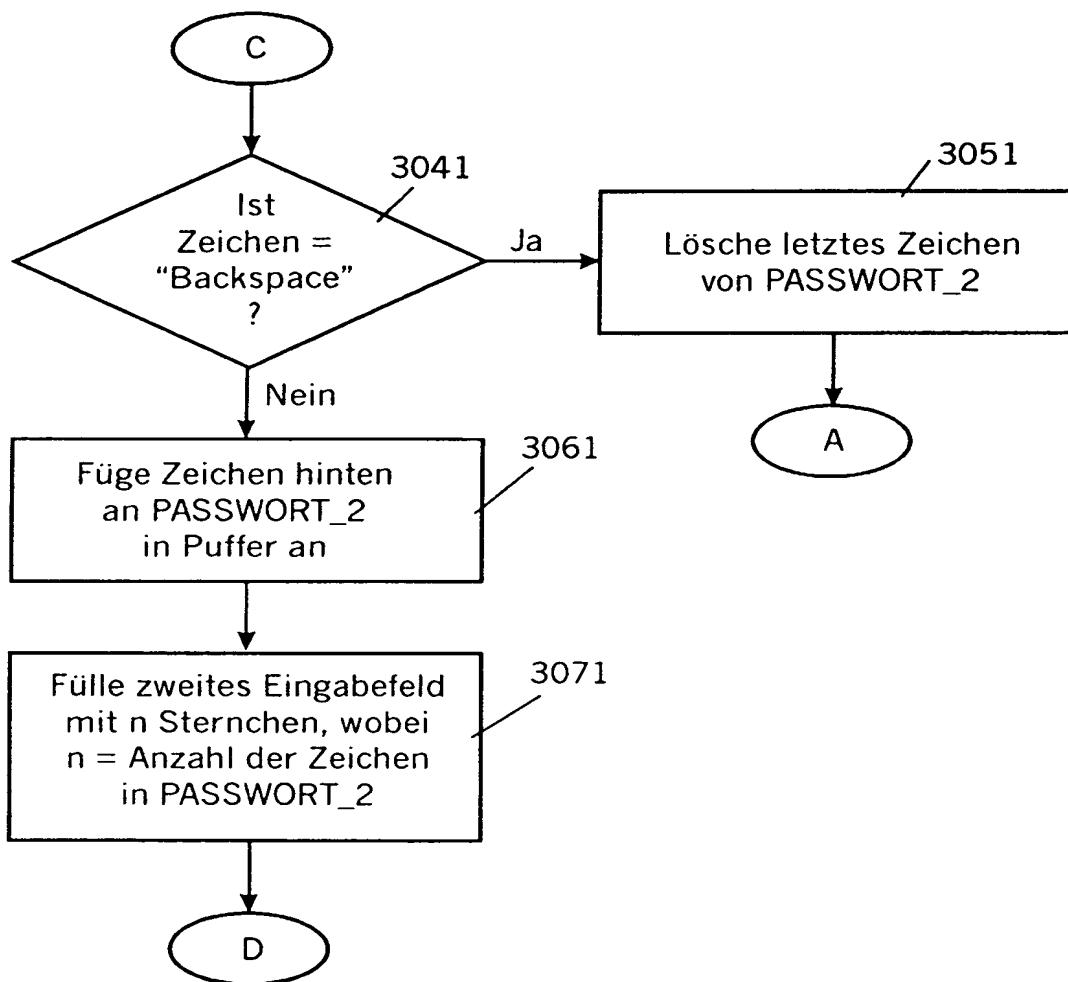


FIG. 3C

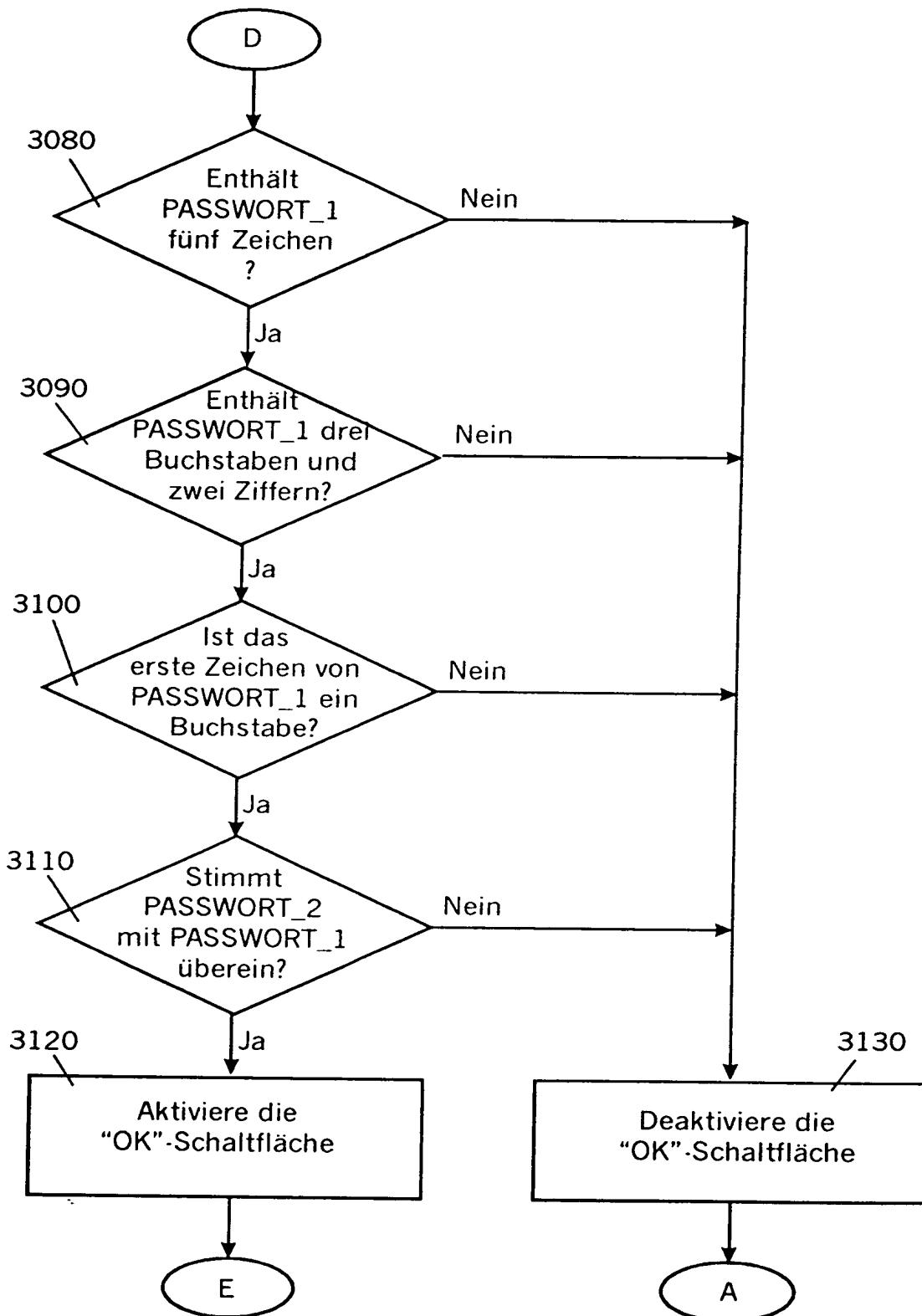


FIG. 3D

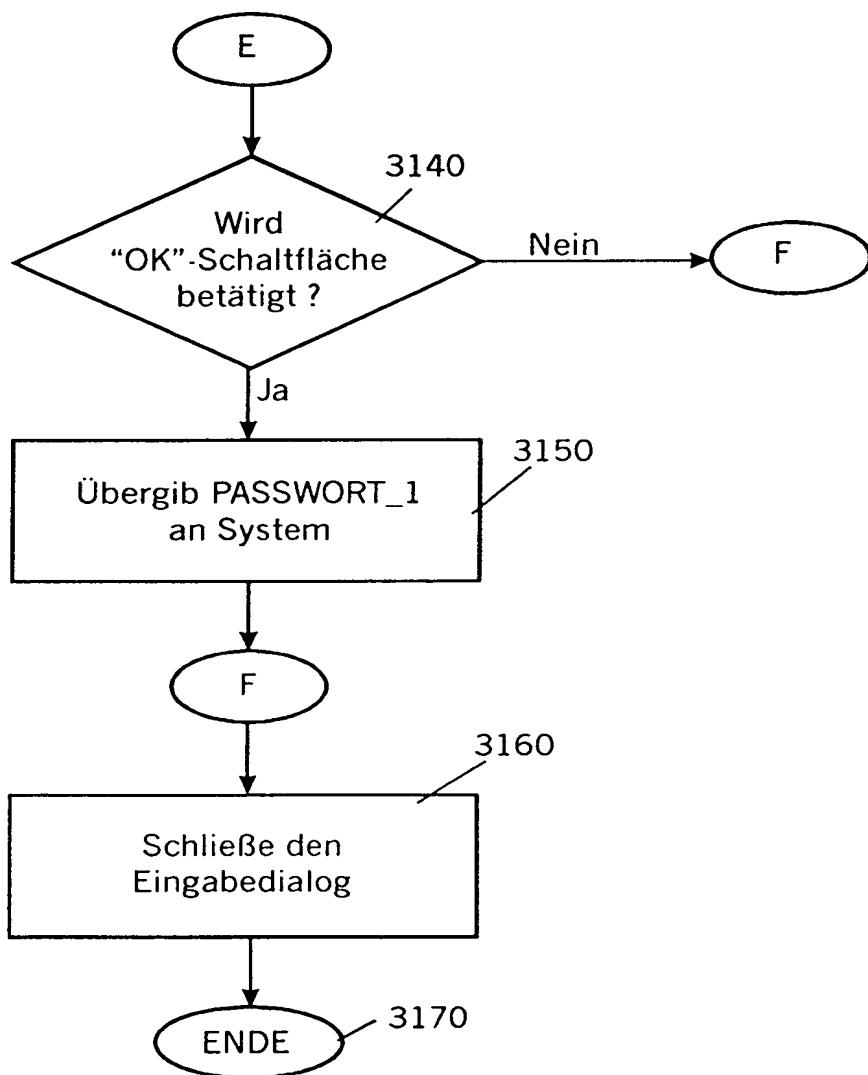


FIG. 3E